

1G-2 IPv6 マルチキャストと IPsec を用いた MPEG2 伝送実験*

大塚玉記[†] 西村浩二[‡] 相原玲二[‡]

[†]広島大学大学院工学研究科 [‡]広島大学総合情報処理センター

1 はじめに

IPv6 [1] は次世代インターネットの通信方式であり、IP ネットワーク上で多地点通信を行なう IP マルチキャスト機能を標準でサポートしている。しかし、有料情報や個人情報等を含む場合、特定の受信者のみが再生できるセキュリティ機能が必要となる。一方、IP レベルのセキュリティ機能として IPsec が一般的になりつつある。そこで今回これらの技術を用いて、約 30km 離れた 2 つのサイト間で MPEG2[2] の伝送実験を行なった。本稿ではその実験内容と IPsec 使用時のスループット、マルチキャスト通信におけるパケット受信時間の揺らぎについて報告する。

2 実験環境

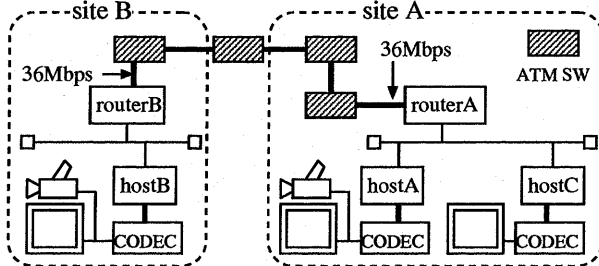


図 1: 実験環境.

表 2: 使用機器.

	hostA,B,C	routerA	routerB
CPU	P3-750MHz	P3-450MHz	P3-550MHz
memory	128MB		
OS	FreeBSD-3.4RELEASE		
KAME	20000605snap		20000619snap

MPEG2 伝送実験における実験環境を図 1, 表 2 に示す。CODEC は沖電気の YS3200 VIDEO CODEC を使用し、MPEG2-TS の出力レートは 6Mbps 固定で行なった。さらに、routerA, routerB 間の転送速度は 36Mbps に設定し、hostA, hostB はマルチキャストの送受信、hostC は受信専用として使用した。マルチキャストルーティン

グ、IPsec の設定に関しては KAME プロジェクト [3] が研究、開発している IPv6 スタック KAME のコマンドを利用した。

3 IPsec 使用時の帯域測定

IPsec は認証ヘッダ (AH)[4] と暗号化セキュリティペイロード (ESP)[5] の 2 つのヘッダを規定している。AH は認証機能を提供し、ESP は暗号化機能を提供する。これらの動作は独立であり、両方を組み合わせて利用することも可能である。

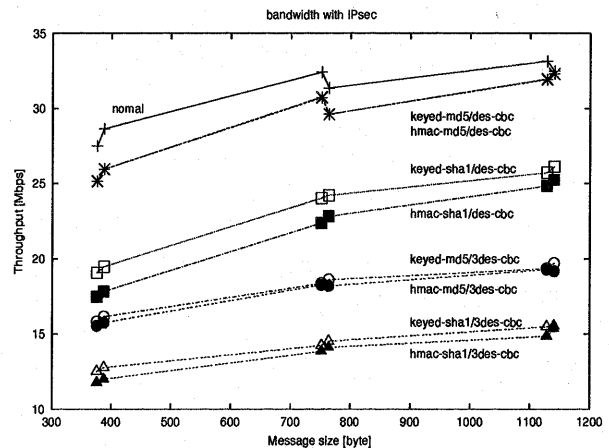


図 3: IPsec 使用時のスループット (hostA → hostB).

AH に対する認証アルゴリズムは hmac-md5, hmac-sha1, keyed-md5, keyed-sha1, ESP に対する暗号化アルゴリズムは des-cbc, 3des-cbc の中から選択する。そして AH, ESP をともに付加した場合の任意のアルゴリズムの組合せに対して、hostA, hostB 間で UDP/IPv6 スループットを測定した (図 3)。図中の normal は IPsec を使用しない場合でのスループットを示している。横軸はメッセージサイズ、縦軸はスループットである。測定には IPv6 対応にした netperf-2.1pl3 を用い、1 回 10 秒の測定を 3 回行ない平均を求めた。図 3 は hostA から hostB への測定結果であるが、hostB から hostA への場合もほぼ同じ

*An MPEG2 transmit experiment with IPv6 multicast and IPsec.

Tamaki Otsuka, Kouji Nishimura and Reiji Aibara

[†]Graduate School of Engineering, Hiroshima University

[‡]Information Processing Center, Hiroshima University

結果が得られた。

4 実験内容

IPv6 マルチキャストによる映像の伝送

マルチキャストによる映像の送受信を行なう。hostA と hostB はマルチキャスト送信をしながら、同時に他のチャンネルを受信できる。hostC は hostA と hostB のマルチキャスト通信を選択的に受信できる。

IPsec の効果

マルチキャスト通信に IPsec(認証と暗号化) を適用することにより、特定の受信者のみが受信可能となるシステムの構築を行なう。認証、暗号化アルゴリズムは keyed-md5, des-cbc を用いる。

5 パケットロスと受信間隔の測定

図1の構成で MPEG2 伝送の実験を行なった結果、映像が一時的に止まる現象がときどき見られた。これは jitter, パケットロス, あるいはプロセスの切替等によるものと考えられる。そこで、hostB から MPEG2 をマルチキャストで送信し、hostA で受信したパケットの到着間隔、パケットロスの測定を行なった。

測定に入る前に OS のタスクスイッチ等の影響を小さくするため、次のことを行なった。

- hostA, および hostB のスワップ領域を使用不可に設定
- 送受信プロセスのリアルタイムスケジューリング優先度を最大に設定

測定方法は次のとおりである。送信側 (hostB) では各パケットにシーケンスナンバを付加して送信する。受信側 (hostA) では各シーケンスナンバをチェックすることによりパケットロスを検出するとともに各パケットの受信間隔も記録する。

パケットの受信間隔について得られた結果を図4に示す。横軸は各パケットに付けたシーケンスナンバであり、縦軸はひとつ前のパケットとの時間間隔を表す。また図中の★印は映像が止まった箇所を示す。測定時間は5分であり、1秒あたり約2000パケットを受信する。また、本測定ではパケットロスについては全く検出されなかった。図4から映像が止まった箇所についてはパケットが大きく遅延しているのが分かる。これは、前述の対策を

とったにもかかわらず、OS のタスクスイッチの影響が出たものと思われる。

また、受信側でコンソールからキーをタイプすることによって図4で見られるような極端な遅延が多く現れ、それに比例して映像の止まる場面が多く見受けられた。したがって、映像の止まる原因はパケットロスではなく、パケットの受信間隔に問題があると考えられる。

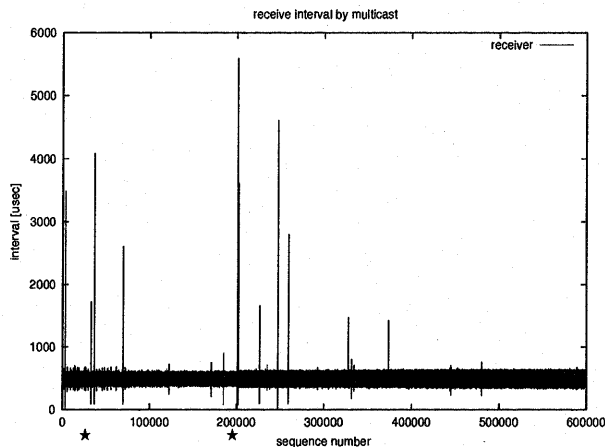


図4: マルチキャストパケットの受信間隔。

6 おわりに

本稿では認証アルゴリズム、暗号化アルゴリズムの違いによる IPsec 利用時のスループットを測定した。そして、マルチキャスト機能および暗号化と認証機能を利用した IPv6 による映像伝送実験を行ない、6Mbps 程度の映像伝送が可能である見通しを得た。映像のマルチキャスト通信におけるパケットの受信間隔、パケットロスを測定したところ、映像の受信はパケットの受信間隔の揺らぎの影響を大きく受けることが分かった。IP ネットワーク上で発生するであろう到着遅延の影響をどのように軽減するかが今後の課題である。

参考文献

- [1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
- [2] 藤原 洋監修. ポイント図解式最新 MPEG 教科書. アスキー出版局, 1994.
- [3] KAME Project, <http://www.kame.net/>
- [4] R. Atkinson, IP Authentication Header, RFC 1826, August 1995.
- [5] R. Atkinson, IP Encapsulating Security Payload (ESP), RFC 1826, August 1995.